



TITLE:

# Construction of new Griesmer codes of dimension 5 (Algebraic System, Logic, Language and Related Areas in Computer Science)

AUTHOR(S):

Inoue, Yuto; Maruta, Tatsuya

---

CITATION:

Inoue, Yuto ...[et al]. Construction of new Griesmer codes of dimension 5 (Algebraic System, Logic, Language and Related Areas in Computer Science). 数理解析研究所講究録 2019, 2130: 109-112

ISSUE DATE:

2019-10

URL:

<http://hdl.handle.net/2433/254755>

RIGHT:

# Construction of new Griesmer codes of dimension 5

Yuto Inoue, Tatsuya Maruta \*

Department of Mathematical Sciences  
Osaka Prefecture University

## 1 Introduction

We denote by  $\mathbb{F}_q$  the field of  $q$  elements. A linear code over  $\mathbb{F}_q$  of length  $n$ , dimension  $k$  is a  $k$ -dimensional subspace  $\mathcal{C}$  of the vector space  $\mathbb{F}_q^n$  of  $n$ -tuples over  $\mathbb{F}_q$ . The vectors in  $\mathcal{C}$  are called *codewords*.  $\mathcal{C}$  is called an  $[n, k, d]_q$  code if it has minimum Hamming weight  $d$ . A  $k \times n$  matrix  $G$  whose rows form a basis of  $\mathcal{C}$  is a *generator matrix* of  $\mathcal{C}$ . A fundamental problem in coding theory is to find  $n_q(k, d)$ , the minimum length  $n$  for which an  $[n, k, d]_q$  code exists for given  $q, k, d$  [5, 6]. The Griesmer bound states that

$$n_q(k, d) \geq g_q(k, d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where  $\lceil x \rceil$  denotes the smallest integer greater than or equal to  $x$ , see [1]. A linear code attaining the Griesmer bound is called a *Griesmer code*. The values of  $n_q(k, d)$  are determined for all  $d$  only for some small values of  $q$  and  $k$  [4, 11]. For the case  $k = 5$ , the following result is well known.

**Theorem 1.1** ([3, 8, 9]). *For any prime power  $q$ ,  $n_q(5, d) = g_q(5, d)$  for*

- (1)  $q^4 - q^3 - q + 1 \leq d \leq q^4 - q^3 + q^2 - q$ ,
- (2)  $q^4 - 2q^2 + 1 \leq d \leq q^4 + q$ ,
- (3)  $2q^4 - 2q^3 - q^2 + 1 \leq d \leq 2q^4 + q^2 - q$ ,
- (4)  $d \geq 3q^4 - 4q^3 + 1$ .

We recently proved the following, which was already known only for  $q \leq 4$ .

**Theorem 1.2** ([7]). *For any prime power  $q$ ,  $n_q(5, d) = g_q(5, d)$  for*

- (1)  $2q^4 - 3q^3 + 1 \leq d \leq 2q^4 - 3q^3 + q^2$ ,
- (2)  $3q^4 - 5q^3 + q^2 + 1 \leq d \leq 3q^4 - 5q^3 + 2q^2$ .

This note is a digest (and some typos are corrected) version of [7].

---

\*Corresponding author. E-mail address: maruta@mi.s.osakafu-u.ac.jp

## 2 Construction methods

Denote by  $\text{PG}(r, q)$  the projective geometry of dimension  $r$  over  $\mathbb{F}_q$ . The 0-flats, 1-flats, 2-flats, 3-flats and  $(r-1)$ -flats are called *points*, *lines*, *planes*, *solids* and *hyperplanes*, respectively. We denote by  $\mathcal{F}_j$  the set of all  $j$ -flats in  $\text{PG}(r, q)$  and by  $\theta_j$  the number of points in a  $j$ -flat, so,  $\theta_j = (q^{j+1} - 1)/(q - 1)$ .

Let  $\mathcal{C}$  be an  $[n, k, d]_q$  code with no coordinate identically zero. Then, the columns of a generator matrix of  $\mathcal{C}$  can be considered as a multiset of  $n$  points in  $\Sigma = \text{PG}(k-1, q)$  denoted by  $\mathcal{M}_{\mathcal{C}}$ . We see linear codes from this geometrical point of view. An  $i$ -point is a point of  $\Sigma$  which has multiplicity  $i$  in  $\mathcal{M}_{\mathcal{C}}$ . Denote by  $\gamma_0$  the maximum multiplicity of a point from  $\Sigma$  in  $\mathcal{M}_{\mathcal{C}}$ . Let  $C_i$  be the set of  $i$ -points in  $\Sigma$ ,  $0 \leq i \leq \gamma_0$ , and let  $\lambda_i = |C_i|$ , where  $|C_i|$  denotes the number of elements in a set  $C_i$ . For any subset  $S$  of  $\Sigma$ , the *multiplicity of  $S$* , denoted by  $m_{\mathcal{C}}(S)$ , is defined as  $m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|$ . Then we obtain the partition  $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$  such that  $n = m_{\mathcal{C}}(\Sigma)$  and  $n - d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}$ . Conversely such a partition  $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$  as above gives an  $[n, k, d]_q$  code in the natural manner. A hyperplane  $H$  with  $t = m_{\mathcal{C}}(H)$  is called a  $t$ -hyperplane. A  $t$ -line, a  $t$ -plane and  $t$ -solid are defined similarly. Denote by  $a_i$  the number of  $i$ -hyperplanes in  $\Sigma$ . The list of the values  $a_i$  is called the *spectrum* of  $\mathcal{C}$ , which can be calculated from the weight distribution by  $a_i = A_{n-i}/(q-1)$  for  $0 \leq i \leq n-d$ , where  $A_j$  is the number of codewords of  $\mathcal{C}$  with weight  $j$ . An  $[n, k, d]_q$  code is called  $m$ -divisible if all codewords have weights divisible by an integer  $m > 1$ .

**Lemma 2.1** ([13]). *Let  $\mathcal{C}$  be an  $m$ -divisible  $[n, k, d]_q$  code with  $q = p^h$ ,  $p$  prime, whose spectrum is*

$$(a_{n-d-(w-1)m}, a_{n-d-(w-2)m}, \dots, a_{n-d-m}, a_{n-d}) = (\alpha_{w-1}, \alpha_{w-2}, \dots, \alpha_1, \alpha_0),$$

where  $m = p^r$  for some  $1 \leq r < h(k-2)$  satisfying  $\lambda_0 > 0$  and

$$\bigcap_{H \in \mathcal{F}_{k-2}, m_{\mathcal{C}}(H) < n-d} H = \emptyset.$$

Then there exists a  $t$ -divisible  $[n^*, k, d^*]_q$  code  $\mathcal{C}^*$  with  $t = q^{k-2}/m$ ,  $n^* = \sum_{j=0}^{w-1} j\alpha_j = ntq - \frac{d}{m}\theta_{k-1}$ ,  $d^* = ((n-d)q - n)t$  whose spectrum is

$$(a_{n^*-d^*-\gamma_0 t}, a_{n^*-d^*-(\gamma_0-1)t}, \dots, a_{n^*-d^*-t}, a_{n^*-d^*}) = (\lambda_{\gamma_0}, \lambda_{\gamma_0-1}, \dots, \lambda_1, \lambda_0).$$

The condition " $\bigcap_{H \in \mathcal{F}_{k-2}, m_{\mathcal{C}}(H) < n-d} H = \emptyset$ " is needed to guarantee that  $\mathcal{C}^*$  has dimension  $k$  although it was missing in Lemma 5.1 of [13]. Note that a generator matrix for  $\mathcal{C}^*$  is given by considering  $(n-d-jm)$ -hyperplanes as  $j$ -points in the dual space  $\Sigma^*$  of  $\Sigma$  for  $0 \leq j \leq w-1$  [13].  $\mathcal{C}^*$  is called a *projective dual* of  $\mathcal{C}$ , see also [2] and [6].

**Lemma 2.2** ([10, 12]). *Let  $\mathcal{C}$  be an  $[n, k, d]_q$  code and let  $\bigcup_{i=0}^{\gamma_0} C_i$  be the partition of  $\Sigma = \text{PG}(k-1, q)$  obtained from  $\mathcal{C}$ . If  $\bigcup_{i \geq 1} C_i$  contains a  $t$ -flat  $\Delta$  and if  $d > q^t$ , then there exists an  $[n - \theta_t, k, d']_q$  code  $\mathcal{C}'$  with  $d' \geq d - q^t$ .*

The code  $\mathcal{C}'$  in Lemma 2.2 can be constructed from  $\mathcal{C}$  by removing the  $t$ -flat  $\Delta$  from the multiset  $\mathcal{M}_{\mathcal{C}}$ . In general, the method for constructing new codes from a given  $[n, k, d]_q$  code by deleting the coordinates corresponding to some geometric object in  $\text{PG}(k-1, q)$  is called *geometric puncturing* [10].

### 3 A sketch of the proof of Theorem 1.2

We constructed a 5-divisible  $[34, 5, 20]_5$  code and a 5-divisible  $[38, 5, 20]_5$  code by some heuristic computer search. Then, we generalized the constructions to the following using a normal rational curve in  $\text{PG}(4, q)$ .

**Lemma 3.1** ([7]). *There exists a  $q$ -divisible  $[q^2 + 2q - 1, 5, q^2 - q]_q$  code  $\mathcal{C}_1$  with spectrum*

$$(a_{q-1}, a_{2q-1}, a_{3q-1}) = \left( \binom{q}{2} + q^4 - 2q^3 + q^2, 3q^3 - 3q^2 + q + 1, \binom{q}{2} + 2q^2 + q \right).$$

**Lemma 3.2** ([7]). *There exists a  $q$ -divisible  $[q^2 + 3q - 2, 5, q^2 - q]_q$  code  $\mathcal{C}_2$  with spectrum*

$$(a_{q-2}, a_{2q-2}, a_{3q-2}, a_{4q-2}) = (q^4 - 4q^3 + 6q^2 - 4q + 1, 5q^3 - 12q^2 + 10q - 3 - \binom{q}{2}, 7q^2 - 9q + 4, \binom{q}{2} + 4q - 1).$$

As projective duals of  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , one can get a  $q^2$ -divisible  $[2q^4 - q^3 + 1, 5, 2q^4 - 3q^3 + q^2]_q$  code  $\mathcal{C}_1^*$  and a  $q^2$ -divisible  $[3q^4 - 2q^3 + 1, 5, 3q^4 - 5q^3 + 2q^2]_q$  code  $\mathcal{C}_2^*$ . It can be also shown that each of the multisets  $\mathcal{M}_{\mathcal{C}_1^*}$  and  $\mathcal{M}_{\mathcal{C}_2^*}$  contains  $q - 1$  skew lines. Applying Lemma 2.2 repeatedly (for  $t = 1$ ), starting with the codes  $\mathcal{C}_1^*$  and  $\mathcal{C}_2^*$ , we get  $[2q^4 - q^3 + 1 - s(q + 1), 5, 2q^4 - 3q^3 + q^2 - sq]_q$  codes and  $[3q^4 - 2q^3 + 1 - s(q + 1), 5, 3q^4 - 5q^3 + 2q^2 - sq]_q$  codes for  $1 \leq s \leq q - 1$ . These provide the Griesmer codes needed to prove Theorem 1.2 when  $d$  is divisible by  $q$ . The rest of the codes required can be obtained by puncturing these divisible codes.

## References

- [1] J. Bierbrauer, Introduction to Coding Theory, Chapman & Hall/CRC, 2005.
- [2] A.E. Brouwer, M. van Eupen, The correspondence between projective codes and 2-weight codes, Des. Codes Cryptogr. **11** (1997) 261–266.
- [3] E.J. Cheon, Y. Kageyama, S.J. Kim, N. Lee, T. Maruta, Construction of two-weight codes over finite fields and its applications, Bull. Korean Math. Soc. **54** (2017) 731–736.
- [4] M. Grassl, Tables of linear codes and quantum codes (electronic table, online). <http://www.codetables.de/>.
- [5] R. Hill, Optimal linear codes, in: Mitchell C. (ed.) Cryptography and Coding II, pp. 75–104. Oxford Univ. Press, Oxford, 1992.
- [6] R. Hill, E. Koley, A survey of recent results on optimal linear codes, in: Holroyd F.C. et al (ed.) Combinatorial Designs and their Applications, pp.127–152. Chapman and Hall/CRC Press Research Notes in Mathematics CRC Press. Boca Raton, 1999.

- [7] Y. Inoue, T. Maruta, Construction of new Griesmer codes of dimension 5, *Finite Fields Appl.* **55** (2019) 231–237.
- [8] Y. Kageyama, T. Maruta, On the construction of Griesmer codes of dimension 5, *Des. Codes Cryptogr.* **75** (2015) 277–280.
- [9] T. Maruta, On the nonexistence of  $q$ -ary linear codes of dimension five, *Des. Codes Cryptogr.* **22** (2001) 165–177.
- [10] T. Maruta, Construction of optimal linear codes by geometric puncturing, *Serdica J. Computing* **7** (2013) 73–80.
- [11] T. Maruta, Griesmer bound for linear codes over finite fields,  
<http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer/>.
- [12] T. Maruta, Y. Oya, On optimal ternary linear codes of dimension 6, *Adv. Math. Commun.* **5** (2011) 505–520.
- [13] M. Takenaka, K. Okamoto, T. Maruta, On optimal non-projective ternary linear codes, *Discrete Math.* **308** (2008) 842–854.